



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/589,177	06/21/2007	Jun Yan	4202-02600	5891
30652	7590	12/24/2009	EXAMINER	
CONLEY ROSE, P.C.			ZIA, SYED	
5601 GRANITE PARKWAY, SUITE 750			ART UNIT	PAPER NUMBER
PLANO, TX 75024			2431	
			MAIL DATE	DELIVERY MODE
			12/24/2009	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/589,177	YAN ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	SYED ZIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 21 June 2007.
- 2a) This action is **FINAL**.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-18 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All    b) Some \* c) None of:
1. Certified copies of the priority documents have been received.
  2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____ .                                    |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ .  | 6) <input type="checkbox"/> Other: _____ .                        |

## **DETAILED ACTION**

This action is in response to the application filed on June 21, 2007. Claims 1-18 are currently being considered.

### ***Priority***

Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) - (d) is acknowledged.

### ***Information Disclosure Statement***

Applicant's IDS form 1449, received on 09/11/2007 and 10/10/2006 has been considered and an initialed copy is attached to this Office action.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim 1-18 is rejected under 35 U.S.C. 102(b) as being anticipated by Kimichi et al. (U.S. Publication No.: 2002/0120760).

1. Regarding Claim 1 Kimichi teach and describe a key distribution method applied in the Next Generation Network comprising a terminal, a soft switch and an authentication center,

comprising: the terminal sending a registration request message to the soft switch for a registration; the soft switch sending the authentication request message to the authentication center for the authentication for the terminal; and the authentication center authenticating the terminal, generating a session key for the terminal and the soft switch, and upon a successful registration authentication, sending the session key to the soft switch so as to be distributed to the terminal (Fig.3c, [0035-0036, 0271-0279, 0384-0396]).

2. Regarding Claim 9 Kimichi reach and describe a key distribution method applied in the Next Generation Network comprising a terminal, a signaling proxy, a soft switch and an authentication center, comprising: the terminal sending a registration request message through the signaling proxy to the soft switch for a registration; the soft switch sending the authentication request message to the authentication center for the authentication for the terminal; and the authentication center authenticating the terminal, generating a session key for the terminal and the signaling proxy, and upon a successful registration authentication, sending the session key to the soft switch so as to be distributed through the signaling proxy to the terminal (Fig.3c, [0035-0036, 0271-0279, 0384-0396]).

3. Regarding Claim 17 Kimichi reach and describe a key distribution system applied in the Next Generation Network comprising: a terminal adapted to send a registration request message for a registration; a soft switch adapted to receive and forward the authentication request message sent from the terminal for the authentication for the terminal; and an authentication center adapted to receive the authentication request message forwarded from the soft switch, to

authenticate the terminal, to generate a session key for the terminal and the soft switch, and to send, upon a successful registration authentication, the session key to the soft switch so as to be distributed to the terminal (Fig.3c, [0035-0036, 0271-0279, 0384-0396]).

4. Regarding Claim 18 Kimichi teach and describe a key distribution system applied in the Next Generation Network comprising: a terminal adapted to send a registration request message for a registration; a signaling proxy adapted to enable the terminal to send the registration request message there though; a soft switch adapted to receive and forward the authentication request message sent from the terminal through the signaling proxy for the authentication for the terminal; and an authentication center adapted to receive the authentication request message forwarded from the soft switch, to authenticate the terminal, to generate a session key for the terminal and the signaling proxy, and to send, upon a successful registration authentication, the session key to the soft switch so as to be distributed through the signaling proxy to the terminal (Fig.3c, [0035-0036, 0271-0279, 0384-0396]).

5. Claims 2-8, and 10-16 are rejected applied as above rejecting Claim 1, and 9. Furthermore, Kimichi teach and describe a countermeasure method, wherein:

As per Claim 2, the step of the authentication center authenticating the terminal comprises: the authentication center generating a first verification word for the terminal according to a key Kc shared with the terminal, encrypting the session key with the shared key Kc, and returning the encrypted session key and the first verification word to the soft switch; the soft switch returning a registration failure response message to the terminal to notify the terminal

of a registration failure; the terminal generating a second verification word according to the key Kc shared with the authentication center, and sending a registration message containing the second verification word to the soft switch for a registration again; and the soft switch authenticating the terminal according to the first verification word and the second verification word ([ 0029-0036, 0271-0279, 0384-0396]).

As per Claim 3, the step of the soft switch distributing the session key to the terminal comprises: the soft switch returning to the terminal a registration success response message containing the session key encrypted with the shared key Kc, and sending a terminal authentication success message to the authentication center; and the terminal decrypting the session key encrypted by the authentication center according to the shared key Kc ([0029-0036, 0271-0279, 0384-0396]).

As per Claim 4, the method further comprises: the terminal sending to the soft switch a list of security mechanisms supported by the terminal and priority information of each security mechanism; the soft switch choosing an appropriate security mechanism for communication according to the list of security mechanisms and the priority information of each security mechanism of the terminal ([0029-0036, 0271-0279, 0384-0396]).

As per Claim 5, the registration request message and the registration message are SIP protocol registration messages, the registration failure response message is a SIP protocol response message, and the registration success response message is a SIP protocol registration request success message; or wherein the registration request message is a system restart message

and a corresponding response message in the MGCP protocol, the registration failure response message and the registration success response message are a notification request message and a corresponding response message in the MGCP protocol, and the registration message comprises a notification message and a corresponding response message in the MOCP protocol; or wherein the registration request message comprises a system service status change message and a corresponding response message in the H.248 protocol, the registration failure response message and the registration success response message are an attribute modification message and a corresponding response message in the H.248 protocol, and the registration message comprises a notification message and a corresponding response message in the H.248 protocol; or wherein the registration failure response message is a gatekeeper rejection message in the H.323 protocol, the registration failure response message is a gatekeeper rejection message in the H.323 protocol, the registration message is a registration request message in the H.323 protocol, and the registration success response message is a registration success message in the H.323 protocol ([0019-0036, 0271-0279, 0384-0396]).

As per Claim 6, the registration request message and the registration message are SIP protocol registration messages, the registration failure response message is a SIP protocol response message, and the registration success response message is a SIP protocol registration request success message; or wherein the registration request message is a system restart message and a corresponding response message in the MGCP protocol, the registration failure response message and the registration success response message are a notification request message and a corresponding response message in the MGCP protocol, and the registration message comprises a notification message and a corresponding response message in the MGCP protocol; or wherein

the registration request message comprises a system service status change message and a corresponding response message in the H.248 protocol, the registration failure response message and the registration success response message are an attribute modification message and a corresponding response message in the H.248 protocol, and the registration message comprises a notification message and a corresponding response message in the H.248 protocol; or wherein the registration request message is a gatekeeper request message in the H.323 protocol, the registration failure response message is a gatekeeper rejection message in the H.323 protocol, the registration message is a registration request message in the H.323 protocol, and the registration success response message is a registration success message in the H.323 protocol ([0019-0036, 0271-0279, 0384-0396]).

As per Claim 7, the registration request message and the registration message are SIP protocol registration messages, the registration failure response message is a SIP protocol response message, and the registration success response message is a SIP protocol registration request success message; or wherein the registration request message is a system restart message and a corresponding response message in the MGCP protocol, the registration failure response message and the registration success response message are a notification request message and a corresponding response message in the MGCP protocol, and the registration message comprises a notification message and a corresponding response message in the MGCP protocol; or wherein the registration request message comprises a system service status change message and a corresponding response message in the H.248 protocol, the registration failure response message and the registration success response message are an attribute modification message and a

corresponding response message in the H.248 protocol, and the registration message comprises a notification message and a corresponding response message in the H.248 protocol; or wherein the registration request message is a gatekeeper request message in the H.323 protocol, the registration failure response message is a gatekeeper rejection message in the H.323 protocol, the registration message is a registration request message in the H.323 protocol, and the registration success response message is a registration success message in the H.323 protocol ([0019-0036, 0271-0279, 0384-0396]).

As per Claim 8, the registration request message and the registration message are SIP protocol registration messages, the registration failure response message is a SIP protocol response message, and the registration success response message is a SIP protocol registration request success message; or wherein the registration request message is a system restart message and a corresponding response message in the MGCP protocol, the registration failure response message and the registration success response message are a notification request message and a corresponding response message in the MGCP protocol, and the registration message comprises a notification message and a corresponding response message in the MGCP protocol; or wherein the registration request message comprises a system service status change message and a corresponding response message in the H.248 protocol, the registration failure response message and the registration success response message are an attribute modification message and a corresponding response message in the H.248 protocol, and the registration message comprises a notification message and a corresponding response message in the H.248 protocol; or wherein the registration request message is a gatekeeper request message in the H.323 protocol, the registration failure response message is a gatekeeper rejection message in the H.323 protocol, the

registration message is a registration request message in the H.323 protocol, and the registration success response message is a registration success message in the H.323 protocol ([0019-0036, 0271-0279, 0384-0396]).

As per Claim 10, the step of the authentication center authenticating the terminal comprises: the authentication center generating a first verification word for the terminal according to a key Kc shared with the terminal and a key Ksp shared with the signaling proxy, encrypting the session key respectively with the shared key Kc and the shared key Ksp, and returning the encrypted session key and the first verification word to the soft switch; the soft switch returning a registration failure response message through the signaling proxy to the terminal to notify the terminal of a registration failure; the terminal generating a second verification word according to the key Kc shared with the authentication center, and sending a registration message containing the second verification word to the signaling proxy to be forwarded to the soft switch for a registration again; and the soft switch authenticating the terminal according to the first verification word and the second verification word ([0029-0036, 0271-0279, 0384-0396]).

As per Claim 11, the step of the soft switch distributing the session key to the terminal comprises: the soft switch forwarding to the signaling proxy a terminal registration success response message containing the session key encrypted by the authentication center respectively with the shared keys Kc and Ksp, and the signaling proxy decrypting with the shared key Ksp the session key encrypted by the authentication center with the shared key Ksp, calculating a message verification word for the registration success response message with the decrypted session key, and forwarding to the terminal the registration success response message containing

the message verification word and the session key encrypted with the shared key Kc; and C6) the terminal decrypting the session key encrypted by the authentication center according to the shared key Kc, and authenticating with the decrypted session key the message authentication word of the message returned from the signaling proxy so as to authenticate an identity of the signaling proxy, an integrity of the message and whether security mechanism parameters of the terminal returned from the signaling proxy are correct ([0029-0036, 0271-0279, 0384-0396]).

As per Claim 12, the method further comprise: the terminal sending to the signaling proxy a list of security mechanisms supported by the terminal and priority information of each security mechanism, and the signaling proxy choosing an appropriate security mechanism for communication according to the security mechanisms supported by the terminal and the priority information of each security mechanism ([0029-0036, 0271-0279, 0384-0396]).

As per Claim 13, the registration request message and the registration message are SIP protocol registration messages, the registration failure response message is a SIP protocol response message, and the registration success response message is a SIP protocol registration request success message; or wherein the registration request message comprises a system restart message and a corresponding response message in the MGCP protocol, the registration failure response message and the registration success response message are a notification request message and a corresponding response message in the MGCP protocol, and the registration message comprises a notification message and a corresponding response message in the MGCP protocol; or wherein the registration request message comprises a system service status change

message and a corresponding response message in the H.248 protocol, the registration failure response message and the registration success response message are an attribute modification message and a corresponding response message in the H.248 protocol, and the registration message comprises a notification message and a corresponding response message in the H.248 a protocol; or wherein the registration request message is a gatekeeper request message in the H.323 protocol, the registration failure response message is a gatekeeper rejection message in the H.323 protocol, the registration message is a registration request message in the H.323 protocol, and the registration success response message is a registration success message in the H.323 protocol ([0019-0036, 0271-0279, 0384-0396]).

As per Claim 14, the registration request message and the registration message are SIP protocol registration messages, the registration failure response message is a SIP protocol response message, and the registration success response message is a SIP protocol registration request success message; or wherein the registration request message comprises a system restart message and a corresponding response message in the MGCP protocol, the registration failure response message and the registration success response message are a notification request message and a corresponding response message in the MGCP protocol, and the registration message comprises a notification message and a corresponding response message in the MGCP protocol; or wherein the registration request message comprises a system service status change message and a corresponding response message in the H.248 protocol, the registration failure response message and the registration success response message are an attribute modification message and a corresponding response message in the H.248 protocol, and the registration message comprises a notification message and a corresponding response message in the H.248

protocol; or wherein the registration request message is a gatekeeper request message in the H.323 protocol, the registration failure response message is a gatekeeper rejection message in the H.323 protocol, the registration message is a registration request message in the H.323 protocol, and the registration success response message is a registration success message in the H.323 protocol ([0019-0036, 0271-0279, 0384-0396]).

As per Claim 15, the registration request message and the registration message are SIP protocol registration messages, the registration failure response message is a SIP protocol response message, and the registration success response message is a SIP protocol registration request success message; or wherein the registration request message comprises a system restart message and a corresponding response message in the MGCP protocol, the registration failure response message and the registration success response message are a notification request message and a corresponding response message in the MGCP protocol, and the registration message comprises a notification message and a corresponding response message in the MGCP protocol; or wherein the registration request message comprises a system service status change message and a corresponding response message in the H.248 protocol, the registration failure response message and the registration success response message are an attribute modification message and a corresponding response message in the H.248 protocol, and the registration message comprises a notification message and a corresponding response message in the H.248 protocol; or wherein the registration request message is a gatekeeper request message in the H.323 protocol, the registration failure response message is gatekeeper rejection message in H.323 protocol, the registration message is a registration request message in the H.323 protocol,

and the registration success response message is a registration success message in the H.323 protocol ([0019-0036, 0271-0279, 0384-0396])..

As per Claim 16, the registration request message and the registration message are SIP protocol registration messages, the registration failure response message is a SIP protocol response message, and the registration success response message is a SIP protocol registration request success message; or wherein the registration request message comprises a system restart message and a corresponding response message in the MGCP protocol, the registration failure response message and the registration success response message are a notification request message and a corresponding response message in the MGCP protocol, and the registration message comprises a notification message and a corresponding response message in the MGCP protocol; or wherein the registration request message comprises a system service status change message and a corresponding response message in the H.248 protocol, the registration failure response message and the registration success response message are an attribute modification message and a corresponding response message in the H.248 protocol, and the registration message comprises a notification message and a corresponding response message in the H.248 protocol; or wherein the registration request message is a gatekeeper request message in the H.323 protocol, the registration failure response message is a gatekeeper rejection message in the H.323 protocol, the registration message is a registration request message in the H.323 protocol, and the registration success response message is a registration success message in the H.323 protocol ([0019-0036, 0271-0279, 0384-0396]).

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz  
November 30, 2009  
/Syed Zia/  
Primary Examiner, Art Unit 2431